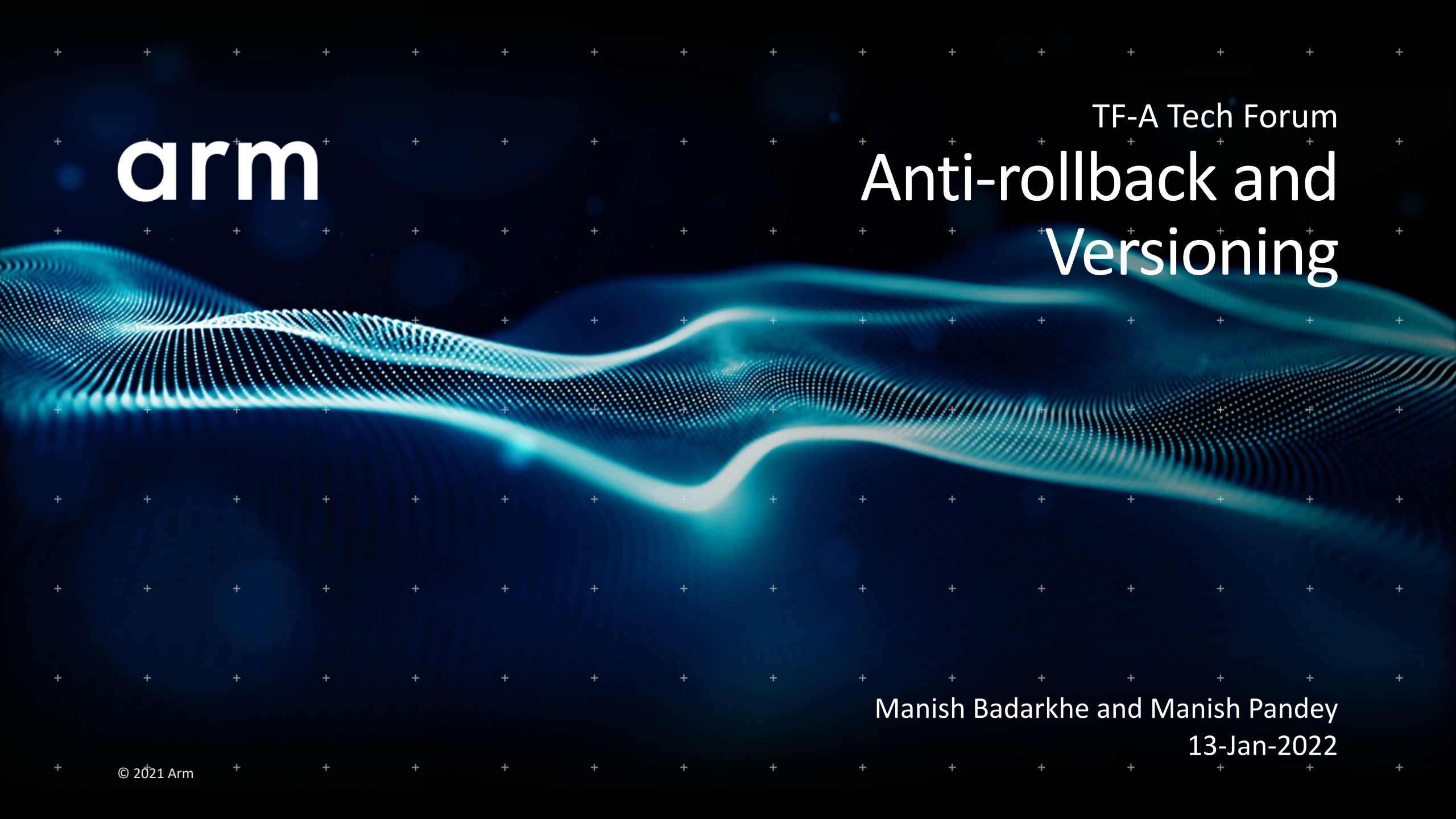


TF-A Tech Forum

Anti-rollback and Versioning

Manish Badarkhe and Manish Pandey

13-Jan-2022

Agenda

- Problem statement - Avoid incrementing Platform NV-counter when updating non-security critical firmware
- In mailing list we explored the possibility of adding FIP version inside FIP header or FWU metadata
  - Next slide discusses about the challenges of this design
- Platform NV counter increment process
  - Existing design
  - Proposed solution

FIP version placement in FIP header or FWU metadata

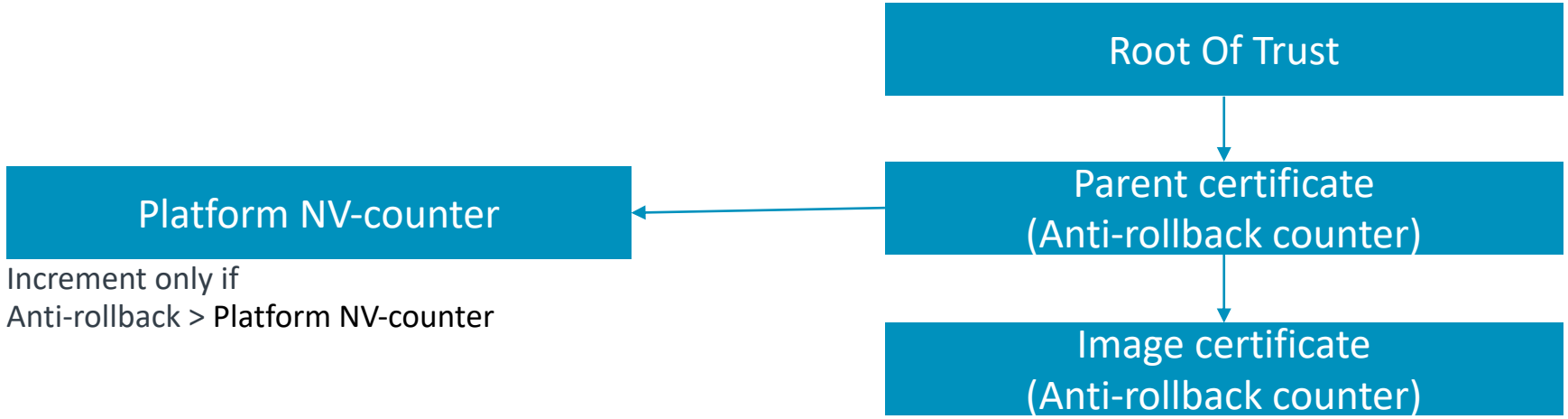
1. Placing version of the FIP inside FIP header
    a. FIP version becomes an un-authenticated field.
    b. It can be used only for sanity checking (ensuring it is in bounded limit).
    c. FIP can be authenticated, but FIP contains mixed images (trusted, non-trusted) then who supposed to sign it? Who will provide FIP version Information?

2. Placing version of the FIP inside FWU metadata
    a. FIP version becomes an un-authenticated field.
    b. FWU metadata authentication is not needed because of below reasons -
        a. FWU metadata integrity check done by the TF-A firmware before consuming it
        b. FWU ABI does not allow update-client to alters the FWU metadata as per the specification
        c. In any case, if FWU metadata gets corrupted then loading the images from corrupted #bank_index leads to authentication failure in TF-A
    c. FWU metadata can be authenticated, but who who supposed to sign it? Who will provide FIP version Information?

Existing Design

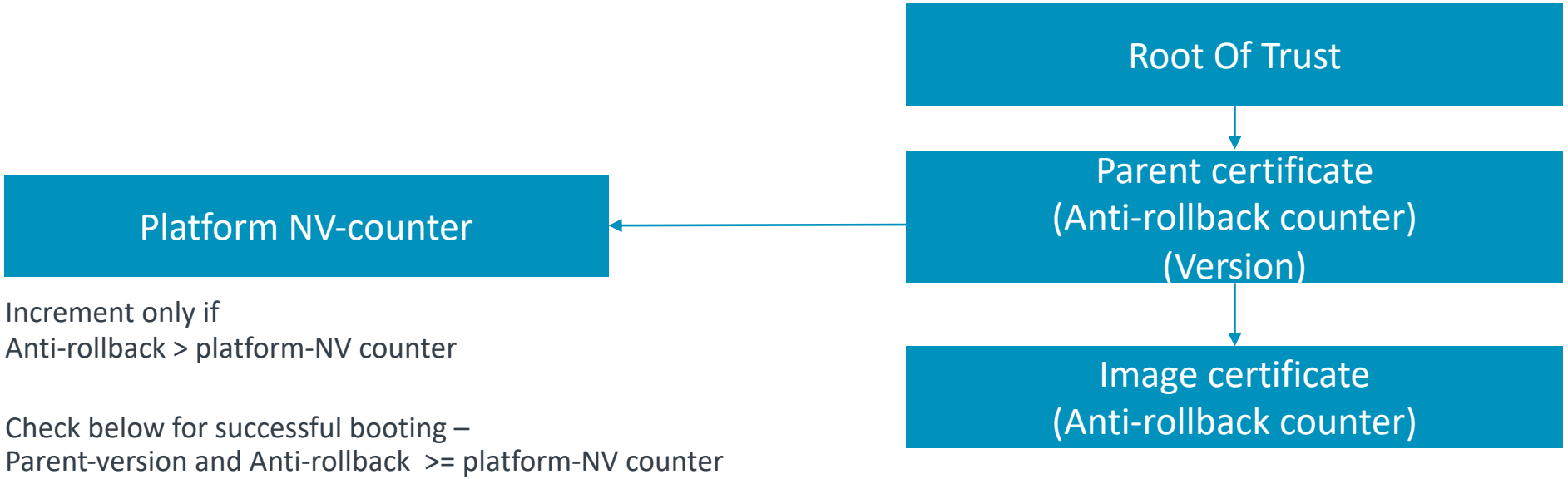
When flash gets written with new firmware by update-agent, on subsequent reboot -

- TF-A firmware starts with trial run –
  - Loads FWU metadata to memory after its integrity check (CRC check)
  - Set boot_index = active_index
  - Do the authentication of the #boot_index images and gives control back to the update-client without incrementing platform NV-counter.
- Update-client and agent accept the image by setting ‘accepted’ flag in FWU metadata
- On subsequent reboot, then TF-A firmware increment the platform NV-counter (if ‘anti-rollback counter’ > ‘platform NV-counter’).



Proposed solution

- In regular run, platform NV-counter gets incremented when anti-rollback counter > platform NV-counter
- It is must to increase the value of the anti-rollback counter value in the certificate when the updates are security-critical
- Solution may be to avoid NV-counter upgrade in regular run (non-security-critical), and to independently increment the version



Thank You
Danke
Gracias
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה